Global Information Assurance Certification Paper

Implementing an Encryption Policy for the Mac OS X User.

by Kenneth Shur

Practical Assignment version 1.3

Summary

Typical courses and discussions on how to use encryption techniques only discuss Windows and UNIX machines. This paper provides the derivation and implementation of a security policy for Mac OS X users.

To my surprise, the Mac OS X user can find a selection of free or low cost solutions for encrypting their valuable data.

Policy Derivation

Once the decision is made to encrypt files on your computer a sequence of events must occur for a secure environment to exist and be maintained. I developed and implemented a personal security policy involving encryption.

When encrypting a file, first select the encryption algorithm. A variety of algorithms are available, each having their own strong and weak points. Some algorithms available are Blowfish, Triple DES, and IDEA. Triple DES is the stronger version of the 56 bit DES algorithm that the U.S. government no longer endorses. If more than one algorithm is used, then the method used must be tracked. Often attributes on the file names indicate which algorithm was used to encrypt the file (.bf for Blowfish for example).

Next determine the encryption key or password and remember what it is. It is highly recommended that the key be recorded in a secure, external location such as a safe. This protects against long term memory loss and enables others to access your files should the need arise. If a variety of passwords are used, then determine a secure method of generating them and maintaining them. A weak password and a known cipher does not give the desired security.

Another area to consider and further investigate is what happens to a file when it is decrypted. Was it disposed of safely? To access an encrypted file, take a strong encryption algorithm and a carefully crafted key and resurrect the clear text. When finished with the clear text file, do not mistakenly think the

© SANS Institute 2000 - 2005 Author retains full rights.

file will be deleted by putting it in the trash and emptying it. Many utilities can recover this data since only the file name is removed from the disk directory, not the data. The disk file must be securely deleted. This is usually done by writing over all of the file's data several times in addition to removing it from the directory.

To go beyond file encryption to include securely transferring or accessing remote files, another set of tools needs to be made available. These tools must not only protect the data transferred but also protect the passwords exchanged when accessing that data.

If security is well integrated, easy to use and, especially for non-engineers, nice to look at, then it will be used. Making a product too unfriendly will keep people from using it.

Security Policy

Purpose - To create a secure system for users of Mac OS X.

Policy -

The applications must be low cost or public domain.
Encryption programs must provide standard encryption algorithms.
Use key lengths that are greater than 56 bits.
Provide a way to track passwords.
No weak passwords will be used.
Provide a way to securely delete files.
Provide secure file transfer and telnet(terminal mode) capability.
Provide secure web access.
All files will be backed up on external media.
All applications used will be backed up. (revision 1)
All applications must be a stable, released version. No beta versions.

Revision History

Added application backup when I found that a file encrypted with one application can not always be decrypted with a different application.

Implementation

A security policy dictates what must be done to ensure a secure system but it also must be one that can be implemented. The products that are used must be available, stable, affordable and useable. Here are some products that will help the Macintosh user achieve these goals for secure file encryption.

File Encryption

PuzzlePalace is an easy to use, shareware application by Brian Hill for OS X that allows the user to encrypt/decrypt files. It gives the user a choice of 5 ciphers (Blowfish, Triple DES, IDEA, CAST or RC5). Users just drag and drop files to and from the application. The program runs very fast but does not have the option of securely deleting the original. If the user double-clicks on the decrypted file icon in PuzzlePalace window the file appears to open without being written to the disk drive. After some investigation, I found a letter from Dana Nau who discovered that PuzzlePlace writes a copy of the encrypted and decrypted file to the /tmp directory. These files are not normally visible to the user except through the command line mode and remain even if the user logs out and logs back in. I verified that it does leave these files in the /tmp directory and that they persist after the user has quit the application and logged out. Hopefully this security flaw is fixed in future versions. I liked the program but cannot recommend it at this time unless this security problem is not a issue. [11]

Crypt is a native Mac OS X shareware application for encrypting and decrypting files with a password of your choice. The cipher used is Blowfish. According to Steve Dekorte, the author, Blowfish is currently the fastest mainstream block cipher and is used in OpenSSH. With that said, I found that Crypt runs about 1/3 of the speed of PuzzlePalace. Even though it runs a few seconds longer, Crypt allows the user the option to delete the original file and also the option to shred it (overwrite it several times with random data). Crypt does not appear to leave files in the /tmp directory as PuzzlePalace does. [1]

My initial policy said to keep track of which algorithm is used to encrypt but it said nothing about which application was used. I found that a file encrypted with Crypt cannot be decrypted with PuzzlePalace and vise-versa. I modified my security policy to always include a backup copy of the applications used for encryption.

An integrated approach was performed by PGP Freeware. This freeware program, available from MIT, incorporates encryption, deletion as well as e-mail support and a VPN client for secure peer-to-peer IP based connections. The program, however, does not support OS X. [3]

The commercial version was available from NAI until they recently announced that they are dropping support for PGP and selling their PGP division.

Tresor is a file and folder encryption application. It takes an arbitrary length passphrase and creates a 160 bit hash using SHA. It then takes 128 bits of this to create the encryption key for the IDEA block encryption. [19]

Secure Delete

For securely deleting files there is ShredIt X, a $19.95 program that shreds files or folders on any writeable media. It lets the user set the number of overwrites and the overwrite pattern.[2] As mentioned earlier, some applications come with a secure delete capability built in.

Northern Softworks makes Trash X, a low cost ($9.95) secure file deletion utility that emulates the desktop trash can. It can secure delete files, folders and disk free space. I would recommend this program for it's functionality and low cost. [17]

SNAX is a file browser that is similar to the Finder but includes a plethora of other features including secure delete. This secure delete overwrites the file three times. [18]

Passwords

There are several ways to keep passwords. OS X provides a utility called Keychain Access or a third party application can be used.

Keychain Access keeps passwords in centralized files. These files are useable on the user's computer and are transportable to other computers. For applications that are "keychain aware", automatic entry of the account and password from the keychain is possible. The keychain can also store encryption keys. Unlike other versions of UNIX that store encryption keys in regular files protected only by file permissions, Keychain Access never reveals the private portion of the key. The private portion of the key cannot be copied either, making it much harder to use the

key on another system. The keychain must first be unlocked in order to take advantage of this service. The passwords are encrypted but I have not been able to determine the method used.

Web Confidential is a $20 application that keeps track of passwords and uses strong encryption (with up to a 448 bit key) to protect them. [16]

When creating a password use at least 8 characters with a mixture of letters numbers and special characters. It's a good idea to run Crack to check the strength of the passwords.

For users that don't want to create their own passwords they can use Northern Softworks Key Cutter, a freeware application that creates strong random passwords that match a user's criteria.

E-mail Encryption

After taking the SANS course and reading their discussion of PGP, I wondered if PGP was available for OS X. PGP allows file encryption as well as verifying a digitally signed file using public/private key encryption. [13]

Mac GNU Privacy Guard, GnuPG, is a free OpenPGP client and is a replacement for PGP. GnuPG does not use the patented algorithm (IDEA). It can be freely used without restrictions which follows the GNU ideal of free software. The GnuPG application is fully RFC2440 (OpenPGP) compliant. [4] Add-ons are available to add functionality such as integration with the native Mac OS X mail application as well as key managers. Using GnuPG is not straight forward or graphical. Not only do you need GnuPG but also several other files to get started.

a) MD5 to verify the signature
b) Entryop Gathering Daemon for generating pseudo-random numbers
c) Easy Install GnuPG for Mac OS X and the Read Me file.

Recently, key management in GnuPG via a GUI was made available in an application called Mac GPG Keys. A beta version is currently available. Because this software is still in beta release, it does not meet the security policy requirement for stable software.

GPGDropThing was freeware created for standard GnuPG services. It allows you to easily encrypt, sign, decrypt and verify text pasted into it's window. This, in combination with GnuPG, can produce an easier to use solution to PGP encryption and decryption.

GPGDropThing and Mac GPG Keys are both available from the Mac GPG Project.

Public PGP key servers are available from places such as PGPnet where users can search for someone's public key or deposit their own public key. Once a key is deposited on a public server, it usually cannot be removed. [10]

File transfer and web

For file transfers and secure web access there are programs that the Mac OS X user will find helpful. Normal FTP transfers and Telnet connections are totally in the clear, including passwords. Secure Shell replaces telnet and sftp replaces plain ftp. SFTP is not FTP over a secure connection. To connect to a server, it must be running a SSH server with a sftp-server.

Mac OS X comes with support for SSH (version 1 and 2) as well as Secure FTP. It also supports being a server. The catch is that it does not have a graphical user interface and the non-UNIX-savy user would not even know it exits. OS X defaults to use SSH instead of Telnet. SSH2 supports encryption using 3DES, Blowfish, CAST128, or Arcfour. For integrity it supports hmac-md5 and hmac-sha1. The user can also forward X11 traffic through an encrypted channel.

Mac OS X version 10.1.3 uses OpenSSH version 3.0.2p1. This release fixes a vulnerability in the UseLogin option of OpenSSH. [14] To read about this vulnerability see reference [15].

The man pages for SSH and sftp that can be accessed via the Terminal program give descriptions on how to use these utilities. Hints on configuring OpenSSH can also be found in reference 12. [5] [12]

A user can execute any command that would be available through the command line interface locally. This means that applications like Netscape Navigator cannot be used but UNIX binaries can.

If using a firewall,open the SSH port 22 instead of Telnet. The disadvantage when using a firewall/filtering router with SSH is the loss of the granularity in what is filtered. Each service has a well known port that is activated to allow that program to operate. With SSH, several protocols can be carried within the encrypted link (such as X11). This means that undesired traffic is allowed to pass undetected by the firewall.

Remote Browser,RBrowser, is a full featured free graphic FTP/SSH/SFTP client. It allows the user to browse local and remote Unix systems and to securely copy files from these systems. This is the last beta cycle before the official release slated for March 10th 2002. Because this software is still in beta release, it does not meet the security policy requirement for stable software. [6]

MacSFTP is a secure ftp application. It supports SSH1 and SSH2. I t uses Diffie-Hellman group1/sha1 key exchange and the standard SSH2 encryption algorithms. It allows drag and drop file transfers and supports AppleScript. A trial application is available for download. Another nice feature is that it allows an interrupted transfer to resume from where it left off. [7]

For Secure X-windows applications there is **eXodus** for $75 from PowerLAN USA. It is a native OS X application that includes a SSH client and is compliant with the X11R6.4 X Window System. [8]

Secure Delete - web & e-mail

I previous discussed the need for securely deleting decrypted files. The same need exists for internet and e-mail traffic.

NetShred allows the user to destroy web browser cache, web browser history and e-mail trash. All of these files would be viewable to any with access to the user's computer since they are not encrypted or securely deleted. This program makes sure that these file types are totally deleted. It fills an important security niche. [9]

Backup

Tri-BACKUP is one of the first OS X backup utilities. It allows the user different choice of backups (mirror, "evolutive", or incremental) and a choice of when to perform the backups (daily, weekly etc.). Another security feature allows for password protection of the compressed archive file. This program smartly provides all of the backup functions a user would need. [20]

Conclusion

Trying to implement a personal computer security policy can be a daunting task with a new operating system. The Mac OS X user can find a selection of free or low cost solutions.

The OS X operating system seems to provide security services that meet many of the security policy requirements. Third party software provides graphical user interfaces and functionality not found in the basic operating system.

I was able to locate software packages that met all of my security policy requirements. Some of the installation and operation may be a bit beyond the beginning user that is not used to command line mode. There does appear to be a constant series of graphical user interface based applications that eliminates or minimizes many of these command line operations, becoming available.

Function	Recommended Application
File Encryption	Crypt
Secure Delete	Trash X & NetShred
Password Management	Keychain Access
E-mail encryption	GnuPG with GPGDropThing
SSH/SFTP/X11	Mac OS X
Backup	Tri_BACKUP

Other places to look for Mac security solutions:

http://www.macsecurity.org/
http://www.openssl.org/
http://www.macintoshsecurity.com/
http://www.macwrite.com/macsecurity/mac-os-x-security-part-5.php
http://www.opendoor.com/macosxalert.html
http://beta.peachpit.com/macsecurity/home.html
http://developer.apple.com/internet/macosx/securitycompare.html
http://www.stanford.edu/group/itss-ccs/security/mac/
http://www.osxgnu.org/
http://senderek.de/security/secret-key.protection.html

References

[1] Dekorte, Steve. "Crypt" URL:
http://www.dekorte.com/Software/OSX/Crypt/ (17 Feb, 2002)

[2] Mireth Technology, "ShredIt X" URL:
http://www.mireth.com/pub/sxme.html (17 Feb, 2002)

[3] MIT distribution center for PGP. "PGP Freeware v6.5.8". URL:
http://web.mit.edu/network/pgp.html (17 Feb, 2002)

[4] Mac GPG Project, "Mac GNU Privacy Guard". URL: http://macgpg.sourceforge.net/ (17 Feb, 2002)

[5] Securemac.com, "Open SSH OS X", URL: http://www.securemac.com/macosxopenssh.php (17 Feb, 2002)

[6] Rbrowser.com Inc, "RBrowser", URL: http://www.rbrowser.com/RBrowser main.html (17 Feb, 2002)

[7] Stierlin, Jean-Pierre, "MacSFTP". URL: http://www.macsecSH.com/ (17 Feb, 2002)

[8] Powerlan USA, Inc. "Exodus". URL: http://www.powerlan-usa.com/exodus.html (17 Feb, 2002)

[9] Mireth Technology, "NetShred" URL: http://www.mireth.com/pub/nsme.html (17 Feb, 2002)

[10] Giger Consulting, "PGP Public Key Lookup Page". URL: http://www.openpgp.net/pgpsrv.html (17 Feb, 2002)

[11] Nau, Dana, User Reviews: URL: http://www.versiontracker.com/moreinfo.fcgi?id=9606&source=sherlock&db=mac (17 Feb, 2002)

[12] Gallop, Damien. "Secure Shell Logins and Mac OS X Part 1". January 11, 2002. URL: http://www.macwrite.com/criticalmass/secure-shell-mac-os-x-part-1.php (17 Feb, 2002)

[13] Gallop, Damien. "Mac OS X Security Part Five: Email Encryption". August 28, 2001. URL: http://www.macwrite.com/macsecurity/mac-os-x-security-part-5.php (17 Feb, 2002)

[14] Wreski, Dave. "OpenSSH 3.0.2 fixes UseLogin vulnerability". December 4, 2001. URL: http://www.linuxsecurity.com/articles/cryptography_article-4107.html (17 Feb, 2002)

[15] Security Focus. "OpenSSH UseLogin Environment Variable Passing Vulnerability". December 21, 2001. URL: http://online.securityfocus.com/bid/3614 (17 Feb, 2002)

[16] Blom, Alco. Web-confidential.com. URL: http://www.web-confidential.com/index.html (17 Feb, 2002)

[17] Norther Softworks. "Trash X". 2001. URL: http://homepage.mac.com/northernSW/trashx.html (17 Feb, 2002)

[18] Cocoatech. "SNAX". 2001. URL: http://www.cocoatech.com/aboutSNAX.html (17 Feb, 2002)

[19] Warlord. "Tresor". URL: http://www.warlord.li/english/tresor.html(17 Feb, 2002)

[20] Tri-edre. "Tri-BACKUP". URL: http://www.tri-edre.com/english/products.html (17 Feb, 2002)